REMARKS

Favorable reconsideration of this application is respectfully requested.

Claims 1-20 are pending in this application. Claims 1-20 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. patent application publication 2003/0007641 to Kinoshita. That rejection is traversed by the present response as discussed next.

Applicants respectfully submit the outstanding rejection is not fully considering all the claimed features relative to the disclosure in Kinoshita. Independent claim 1 recites "a second identification information generator which generates second identification information including the service name, the inherent information and the encryption data", the encryption data including encrypted "first identification information including a service name of available service and inherent information". Independent claim 18 recites similar limitations. Thereby, in independent claims 1 and 18, and claims 2-6 dependent therefrom, the second information includes (1) a service name and inherent information (which is ***not*** encrypted) and (2) data with the ***encrypted*** service name and inherent information.

Claims 7-17 and 19 recite determining whether a communication partner is trustworthy based on a result of comparing data obtained by decrypting encryption data included in first identification information with the service name and the inherent information included in the first identification information.

In such ways claims 1-6 and 18 are directed to a transmission side and claims 7-17 and 19 are directed to a reception side. Claim 20 is directed to a configuration of both transmission and reception sides.

In the claims, a transmission side transmits encryption data obtained by encrypting a service name and inherent information, and additionally transmits, without encryption, the service name and the inherent information. A reception side can determine whether a result of decrypting the encryption data coincides with the also received service name and inherent

information, and can thereby determine whether the transmission side is trustworthy. That is, according to operations that can be realized in the claimed invention, as a transmission side transmits encryption data obtained by encrypting a service name and inherent information, in addition to transmitting the service name and inherent information without encryption, the reception side can easily and accurately determine whether the transmission side is trustworthy.

If it is assumed that the transmission side transmits only the encryption data and the encryption data has been generated by using a secret key that the transmission side improperly acquired, the reception side may erroneously determine that the transmission side is trustworthy without noticing the improper acquisition of the secret key. Even when the transmission side transmits non-encrypted service name and inherent information, the reception side cannot determine whether the transmission side improperly acquires such information.

The claimed inventions can address such a situation since in the claimed inventions encryption data obtained by encrypting a service name and inherent information is transmitted in addition to transmitting the service name and the inherent information, without the encryption. Thereby, a reception side can confirm that the service name and inherent information are correct and confirm that the correct service name and inherent information are included in the encryption data. Thus, the claimed inventions allow more accurately determining the credibility of a communication partner.

Applicants submit the claimed features clearly distinguish over Kinoshita.

The outstanding rejection is misconstruing the teachings in Kinoshita in that Kinoshita does ***not*** disclose or suggest communicating information including ***both*** data with an encrypted service name and inherent information and the service name and inherent information itself, i.e. which has not been encrypted. As is clear from the operation shown in

Figure 7 in Kinoshita the first information exchanged is key data (operation 72), which allows the generation of encrypted data (operation 74), so that thereby data encrypted using the key data can then be exchanged (operation 75). Thereby, from that operation it is clear that in Kinoshita the only information communicated is key data and data ***encrypted*** with the key data. Kinoshita in that respect does ***not*** disclose or suggest any transmission of (1) a ***service name and inherent information*** and (2) data with the encrypted service name and inherent information.

Kinoshita also cannot realize benefits in the claimed invention by virtue of such differences between the claimed invention and Kinoshita.

More specifically, in the device such as Kinoshita only encryption data obtained by encrypting a service name and inherent information is transmitted. Thereby, if an unauthorized person uses a secret key improperly acquired and improperly encrypts a service name and inherent information, the unauthorized person may encrypt and transmit an arbitrary service name and inherent information by using the improperly acquired secret key without any authorization. In such a case a receiver side may acknowledge any service name and inherent information as valid information because such information is encrypted by a specified secret key.

In contrast to such operations in Kinoshita, in the claimed invention since both of an encryption data and data before being encrypted is transmitted, even if an unauthorized person improperly encrypts the service name and inherent information by using the improperly acquired secret key, a receiver side can detect an invalidation by confirming a confirmation of validation using the service name and the inherent information that is transmitted but that has not been encrypted, and by comparing such with a service name and inherent information as encrypted in the encryption data. Thereby, an improper service name and inherent information will not be recognized as valid information.

Kinoshita does not disclose or suggest such features. Kinoshita merely discloses key data for both encryption-decryption is used to encrypt and transmit data. Such an operation in Kinoshita is a standard operation to encrypt data that is to be transmitted. In contrast to Kinoshita, in the claims the encrypted service name and inherent information are transmitted with the service name and inherent information without encryption, which is neither taught nor suggested by Kinoshita, and which has not been fully recognized in the Office Action.

The outstanding grounds for rejection cites Kinoshita at paragraphs [0035]-[0040] with respect to the above-noted claim features, but such disclosures in Kinoshita do not correspond to the claim features. Those disclosures in Kinoshita are directed to the operation in Figure 7 discussed above, in which Kinoshita discloses exchanging key information and then transmitting data encrypted with the key information. In that respect Kinoshita specifically states "[t]he transmission/reception module 23 supplies the data ***encrypted*** by the unit 22 to the antenna 21, which transmits the data to the station 3 (Step 25)".[1] From that disclosure it is clear that in Kinoshita the only data transmitted is data encrypted by the encryption key, and in that respect Kinoshita clearly does ***not*** disclose or suggest additionally sending the service name and inherent information itself, i.e. which has not been subject to the encryption.

Also, at paragraph [0040] Kinoshita discloses key data is exchanged and SDP (Service Discovery Protocol)-service search request is performed. In that respect Kinoshita's search is only for the services, and does not even verify the validity of the services. Thereby, Kinoshita does not even recognize the problem solved by the present invention of preventing unauthorized use of a service name.

[1] Kinoshita at paragraph [0036]. (Emphasis added).

In view of the foregoing comments, applicants respectfully submit the claims as currently written positively recite features that distinguish over Kinoshita. Thereby, each of claims 1-20 as currently written is believed to be allowable over the applied art.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870
Surinder Sachar
Registration No. 34,423

EHK:SNS\la

I:\ATTY\SNS\24's\244986\244986US-RESPONSE.DOC